LEGAL ASPECTS OF ICE-PICK TESTING

Dr. Bruce C. Gabrielson
Kaman Sciences Corp.
Alexandria, VA

in Association with Naval Research Laboratory
Contract No: M00014-93-C-2033

Abstract

The Ice-Pick package is a window driven program that provides a multi-layered approach to network testing. The automated tool is used to identify frequently exploited security problems present on well known UNIX based operating systems. Information provided by testing is used to determine what protective mechanisms need to be implemented by network administrators.

The paper deals with two issues of primary concern, the user's legal basis for performing vulnerability identification testing, and the consequences of unauthorized use or release of the software itself. It is essential for self protection that the tester understands what he or she can legally do with a tool such as Ice-Pick. The issue of trust can also effect users. Trusting each user to protect Ice-Pick against unauthorized release is essential for absolute control of the technology involved.

The structure of this document allows traceability from top level law through applicable Navy regulation. The most important points are the understanding of what monitoring involves, and knowing what the Ice-Pick test tool can be used for. The use of other penetration type testing tools, such as SATAN, will not be discussed, nor will the regulatory requirements of non-Navy organizations. However, the discussion can be applied to using similar test tools in other organizations.

Introduction

This paper discusses the legal basis for performing Ice-Pick testing in the Navy, and the consequences of unauthorized use or release of the software itself. It is essential for self protection that the tester understands what he or she can and can't do with the tool. Providing the information background for the tester to evaluate test activities is one means of accomplishing affective conditioning. Therefore, the legal basis supporting testing and accountability when using the tool will be derived first.

Trusting the user is another issue. Although trust of each user against the unauthorized release of Ice-Pick is assumed, its distribution must be absolutely controlled. Therefore, a discussion of the repercussions of improper release, particularly to the user, will enhance the user's awareness of the problem, as well as provide the legal basis for prosecution should the software find its way into the wrong hands.

Background on Ice-Pick

Ice-Pick is an unclassified automated tool that can be used for testing network vulnerability profiles. The Navy developed it to proactively attack its own networks for SST&E purposes. Ice-Pick does what it is intended to do very well. The Ice-Pick user can only test for vulnerabilities. Private information can not be accessed with the Ice-Pick application running.

Ice-Pick's software incorporates protection mechanisms to ensure only pre-authorized sites will be targeted. The software can also be directed to run on only one pre-designated machine. However, these controls are directed at software operation. Using the program requires a certain level of technical skills. The skills required are information sensitive in nature in that the individual using the program could basically become an accomplished "hacker".

The problem with the deployment of a proactive test tool is that it is capable of being used both for and against a network. Ice-Pick is simply a tool which has a number of internal program safeguards, and also needs a certain level of expertise to be used properly. Since it relies on applying technologies that could be misused, the tester needs to fully understand both regulation and capability in order to correctly apply tests where they may be legally be used.

General Legal Policy

Formal adherence to detailed security standards for electronic information processing systems are necessary for industry and government survival. These security standards are necessary because of the amount of information, the value of the information, and ease with which the information can be manipulated or moved. However, standards must be backed by law if they are going to be mandated. Government organizations are required to comply with these laws, as well as comply with numerous regulations related to unclassified sensitive and classified environments. Each organization has, therefore, developed its own set of instructions regarding how it will comply with top level laws and requirements.

Top Level Legal Traceability Issues

Two federal laws drive the need for protecting an organization's network and computing resources. The National Computer Security Act requires computer security implementation and training on Government computers in order to provide for information protection. The second law, the Privacy Act, protects private information on individuals. Government organizations should be in full compliance with these and other security or privacy type regulations. In addition, Department of Defense organizations have issued site specific instructions regarding the protection of their sensitive, but unclassified information. Penalties for the unauthorized release of protected information, as well as specific access authorization criteria are well documented.

There is also a personal liability issue. Down time to get an organization's network back on-line, or to simply recover data after a virus attack can be very expensive. Costs can also be high if certain types of data is manipulated to show other than actual information. Therefore, it is important for the tester to understand that unauthorized use of any software for the purpose of manipulating or otherwise destroying data can result in personal legal responsibility for organizational financial loss.

Privacy Act and Federal/Public Law

The top level Federal Statute relating to private information of an individual citizen is covered under the Privacy Act of 1974. This law protects individuals from disclosure of various categories of information, and has significant penalties imposed on violators. A important provision of the Act is shown below:

> ***Privacy Act of 1974 (as of Jan 1993)***
>
> ***552a. Records maintained on individuals***
>
> *(b) Conditions of disclosure.--No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be-- (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties; ....*

Two other laws have a direct bearing on those who are responsible for protecting computer assets.

> ***Public Law 100-235*** *(Computer Security Act) is intended: "To provide for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes."*
>
> ***OMB Circular A130*** *Federal ADP guidelines. "The Paperwork Reduction Act (44 U.S.C. Chapter 35) assigns the Director of the Office of Management and Budget (OMB) responsibility for maintaining a comprehensive set of information resources management policies and for promoting the application of information technology to improve the use and dissemination of information by Federal agencies."*

Network Monitoring and Privacy

How are privacy and network monitoring related? When dealing with a computer tool, several items are considered. For example, will using the tool result in keystroke monitoring or packet detection, or will it allow real-time communications detection. Related to electronic monitoring, privacy rights are found in the Electronic Communications Privacy Act of 1986, and are embedded in the US Constitution. The Electronic Communications Privacy Act of 1986 (ECPA) provides additional privacy protection against monitoring. Title I of the ECPA includes electronic communications and its protection. Title II of the statute protects stored communications. The Fourth Amendment of the Constitution provides that:

> *"the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrants shall issue, but upon probable cause,..."*

As indicated, compromising one's privacy is a serious issue, requiring both a formal process and probable cause. In other words, legal action is necessary to compromise an individuals privacy.

Accessing Stored Communications

Both real time and stored communications could be considered private. Section 2701 of Title 18 of United States Code makes it a criminal offense to unlawfully access stored communications. It is a violation of this section to intentionally access without authorization a facility through which an electronic communication service is provided; or to intentionally exceed an authorization to access that facility and thereby obtain, alter, or prevent authorized access to a wired or electronic communication while it is in electronic storage in such systems. This is a criminal statute and fines and imprisonment can result.

Relevant Laws/Acts/Circular

PL 97-255
Federal Managers Financial Integrity Act of 1987
PL 99-473
Comprehensive Crime Control Act of 1984
PL 99-474
Computer Fraud & Abuse Act of 1986
PL 100-235
Computer Security Act of 1987
PL 100-503
Computer Matching and Privacy Protection Act
OMB Circular A-130
Mgt. of Federal Information Resources
OMB Circular A-123 & 127
Internal Control/Financial Management Systems

Other Relevant Documents

OMB Bulletin 89-22
OMB Bulletin 90-08
EO 12333
EO 12356
DCI DIR 1/16
US CODE, TITLE 18, SECTION 2511

Applicable Defense Statutes (Navy Example)

DOD 5200.28-STD (Orange Book)
OPNAVINST 5239
SECNAVINST 5239
SITE INSTRUCTION

If an individual has a reasonable expectation of privacy in his or her computer (hardware or software), there must be some legal safeguards put in place before a search and seizure of the computer or communications can take place. If the action is part of a criminal investigation, then a warrant is required. Note that even in situations where government employers or supervisors seek access to an employee's computer (or office, desk, etc.) there must be, in the absence of a warrant, a reasonableness determination and a balancing of the employee's privacy interests that will withstand judicial scrutiny. Determining what level of constitutional protection a government employee has in a work-setting depends on the circumstances and whether the employee has a reasonable expectation of privacy.

On the issue of reasonableness, one issue of privacy relates to the practice of network monitoring by individual Government organizations. Neither a warrant nor a reasonableness determination is required where there is no reasonable expectation of privacy, or where the individual has consented to intrusion. Within the Department of Defense, all DoD interest computer systems and related equipment are intended for the communication, transmission, processing, and storage of official US Government authorized (and owned) information only. US Government telecommunications systems and information systems (ISs) are subject to periodic security testing and monitoring without prior notification to ensure proper functioning of equipment and systems including security devices, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. Use of any Government network or equipment constitute consent to monitoring.

Monitoring notices indicating that there is no right to privacy in the system by any user is advantageous relative to reasonableness. Some Government agencies (such as the Navy) have complete control over their network and include a monitoring notice such as that shown below which appears every time a user logs onto many networks.

> *"All Department of Defense telecommunications and automated information systems are for the communication, transmission, processing, and storage of U.S. Government information only. The systems and equipment are subject to authorized monitoring to ensure proper functioning, to protect against unauthorized use, and to verify the presence and performance of applicable security features. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel. Anyone using this system expressly consents to such monitoring."*

Unfortunately, implied consent isn't always accepted by an employee. In addition, not every organization can claim they have the legal right to gain access to an individual's personal files. Since testing may result in the identification of an access point, one of the initial concerns a testing organization has is their legal basis for testing.

Lets examine closely what a penetration test tool really does. Remember that these tools work by actually attacking a network. If the attack is successful, it can also be used as an initial step in the monitoring process. Public Law 99-474 applies to those who knowingly access a computer without authorization, or to those who exceed their authorization. Additionally, although the site users are normally pre-warned, the actual testing of a particular user's machine must be accomplished with sensitivity to both the user and the system manager responsible for the network being tested to avoid any misunderstandings.

There also may be site/organization specific legal issues in accessing sensitive non-classified information which may include private information. However, informed consent of the user (the login banner) minimizes legal issues presented to the system administrator by using tools such as Ice-Pick. An organization should not perform network testing until it can certify that 100% of the computers to be tested display the proper monitor banner. Additionally, some system administrators choose to use a formal users agreement which lays out the same type of information contained in the banner, and contains the user's signature acknowledging an understanding of the banner.

In spite of the implied consent provided by the use of login banners, understand that formal computer monitoring is allowed only in very limited situations and only when pre-approved at the appropriate level. For the Department of Defense, Communications Security (COMSEC) monitoring is under the cognizance of the National Security Agency, who then delegates to service cryptological elements.

Use Within the DoD

The Computer Security Act established the guidelines and rules for the protection of Government computing assets. Within the Department of Defense (DoD), security rules have been established to implement the Computer Security Act and protect computer systems which process classified or sensitive but unclassified information. These rules are intended to provide guidance for both manufacturers and for users. Computers that meet the National Computer Security Center's (NCSC's) trusting criteria have integrated safeguards into their operation such that only the users "trusted" to have access to the restricted data can actually gain access.

The rules are described in a series of documents known as the Rainbow Series. Currently there are six levels of Trusted Computer classifications as described in the Orange Book[1]. Requirements for software/hardware security policy, accountability, assurance, and documentation vary depending on the level of security to be achieved.

From the initial Rainbow Series documents, various DoD organizations established and developed their own programs to implement information security rules.

Navy Regulations/Instructions

The Navy's computer security program structure followed the guidelines established by DoD 5200.28, plus has incorporated the requirements of newer laws and directives, including the Privacy Act. The Navy's current program is based on the requirements of SECNAVINST 5239.3 dated 14 July 1995. Policy will be further implemented by the OPNAVINST 5239.X currently in draft form. Specific to the type of protection addressed by Ice-Pick testing, the following paragraphs relate directly, with bold type indicating the specific wording:

[1] ***Trusted Computer System Evaluation Criteria, DoD "Orange Book", DOD 5200.28, DECEMBER 1985.***

SECNAVINST 5239.3

"7. Policy"
"b. Fundamental INFOSEC Policy"

"(1) Data processed, stored and transmitted by information systems shall be adequately protected with respect to requirements for confidentiality, integrity, availability and privacy."

"(2) The nature of the DON mission, accompanied by connectivity and data aggregation issues, has led to the determination that all unclassified information processed by DON information systems is sensitive. ***Therefore, all DON information systems shall be protected by the continuous employment of appropriate safeguards."***

IS Security Program Implementation

The Information System (IS) Security Program developed by Government organizations is designed to provide end-users with good security practices as well as comply with current Government requirements. This practice establishes good habits within the local community and narrows the possibility of: disclosure of data, equipment loss, and misuse of government resources.

The Navy's IS Security Program is designed to ensure the confidentiality, integrity, and availability of its computing assets. It is driven by a primary need. The need to maintain configuration management controls over equipment that may be susceptible to identified threats.

The potential risks to Navy computers posed by potential threats establishes the basis for controlling the configuration management of all IS which process classified and unclassified but sensitive information. The Navy has chosen to address this control need through the establishment of a Risk Management Program, which in turn requires a verification process to ensure its viability.

The ultimate recognition of the potential hacker/cracker threat beyond the stand-alone IS has resulted in an expansion of the risk management program as well as the implementation of a network oriented security system testing & evaluation (SST&E) program.

Navy networks are constantly bombarded by off-site hacker/cracker penetration attempts. In the Navy's network monitor and test role, an active evaluation, test, and continual upgrade of network security protection measures are necessary throughout the IS's life cycle.

Security System Test and Evaluation

The SST&E function is the active auditing part of the Navy's IS security configuration management procedure. SST&Es gather empirical data on individual systems and are examined by the DAA in the evaluation procedure. Applying the SST&E process to the active testing of networked ISs provides the local IS Security Group with the ability to protect Government computing resources under its control. The process evaluates the effectiveness of in-place countermeasures against incidents that would effect the networked IS in a negative manner. If the in-place countermeasures are inadequate, the SST&E will uncover this fact so they can then be rectified.

SPAWAR Security Program Compliance

Within the Navy, the Chief of Naval Operations (CNO) has appointed the Director, Space and Electronic Warfare, as the Navy's Senior Information Systems Security Manager (SISSM). Among the SISSM's tasks are maintaining the OPNAVINST 5239.X and its supplements, and maximizing the use of automated security related tools. As the following document describes, Ice-Pick is considered by name as one of these tools.

> ***Automation in Certification and Accreditation, SPAWAR PD 51, Section 2.0 Automation Support for the Naval Systems Security Engineering Process***.
>
> ***"2.1.6 Secure System Operation"***
>
> ***"The system security personnel must be able to maintain and monitor system operation and determine the security effectiveness of the installed system. .... During operation, the system security personnel need to be able to probe the system, control system access and usage, and understand the impact of system configuration changes to the system security.***"
>
> ***"2.3 AUTOMATION OBJECTIVES***"
>
> *"Specific activities within the security engineering process that are suited to automation are listed below:"*
>
> ** Conduct security testing (i.e., Certification Test & Evaluation [CT&E], Security Test & Evaluation [ST&E]) in conjunction with normal system testing activities; support covert channel analysis,* ***penetration testing,*** *and operational testing."*
>
> ***"7. Policy"***
> ***"b. Fundamental INFOSEC Policy***"
>
> ***"Section 6: Recommendations"***
>
> *"Finally, for the long-term, the study team recommends that SPAWAR PD 51 pursue the analysis and application of certain classes of tools. These include ......* ***tools that enable the ISSO/SA to monitor, probe, and analyze the security posture of an operational system (e.g., ISS, Icepick)."***

Why is Ice-Pick's Use Acceptable

Ice-Pick, when properly used as an integral part of a network vulnerability protection program and is fully compliant with relevant individual privacy safeguards. It is not considered to be computer monitoring (in the legal sense) because it does not involve either real time wire interceptions, nor does it access stored communications. Since it's use could present a 4th Amendment privacy concern, it is essential that the tester has the consent of those to be tested. Therefore, to protect both the tester and the test organization, formal authorization to test, signed by the appropriate authority must be obtained prior to testing, and all systems to be tested must have a security banner regarding expectation of privacy. The following basic model is recommended when a site is to be tested.

1. Identify the point of contact (usually the DAA) of the organization.
2. Get written permission from the point of contact to perform the vulnerability analysis
3. Notify system administrators on the target network (if appropriate)
4. Ensure that you properly select the approved specific target for testing
5. Do the vulnerability analysis (test)
6. Report all results to the organization's point of contact
7. Protect or destroy all vulnerability data collected still in your possession (as appropriate*)

*Ice-Pick has the ability to archive some test related information. If the tester is testing the site where he is employed and under direct supervision of the DAA, the data collected can be archived. If the tester is testing another organization's site, all vulnerability data should be delivered with no data archived.

The local site may also have an audit type monitoring tool requirement imposed on network test activities. This control function would then automatically provide a check on the testers activities as well as protecting the test authorizing organization from access liability. If such an audit tool is required, it is become the responsibility of the host organization to provide it to the Ice-Pick tester.

Inappropriate Use of Government Resources

What can happen to a tester if Ice-Pick is used in an unauthorized manner? Accessing, manipulating or otherwise using Government owned or leased equipment in an unauthorized manner, or on Government time, will be considered a misappropriation of public resources. Further, it is contrary to published Navy policy. If routine monitoring by the IS Security organization reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If auditing or monitoring reveals violations of security regulations of unauthorized use, employees who are responsible may be subject to appropriate disciplinary action. The burden of responsibility rests directly on the user's shoulders should a potential legal issue develop later during an actual test.

Release Concerns

Predicting what would happen if a new vulnerability test tool was released without controls is difficult. Judging by what has transpired relative to the issuance of security advisories when similar programs were released, at the very least network attacks could noticeably increase. However, Ice-Pick's first line of defense is its internal program safeguards. The application is limited internally before distribution to pre-coded net masks.

The second line of defense relates to the trust safeguard. Unlike other available test tools, the Ice-Pick program is U.S. Government property and is strictly controlled for Official Government Use Only. Unauthorized use, distribution, reproduction, or possession may be grounds for criminal prosecution including imprisonment. As custodian of the Ice-Pick software, it is the user's responsibility to protect it.

How can user culpability be ensured? Through the use of training. Ice-Pick training covers applicable legal requirements as well as proper procedures and controls for tool application. Such manditory training is also intended to reduce the possibility of accidental misuse as well as instill the importance of maintaining strict control of the software package.

The complete Ice-Pick package is a powerful security tool, useful for the system administrator to identify and fix potential vulnerabilities in Navy networks. If not protected, it could prove to be as useful to an unwanted perpetrator.